# *Security Considerations for the Future e-Enabled Aircraft*

**Dr. Chris Dhas**

**Chris A. Wargo**

**e = IP**

**ICNS Aerospace**

**May 22, 2003**

7405 Alban Station Court, Suite B225, Springfield, Virginia 22150-2318 (703) 644-2103

www.CNSw.com

# *Paper Contents*

- Introduction
- Review of threats and impacts
- Review of available security mechanisms for Internet applications
- Review of available security mechanisms for Aeronautical Telecommunications Network(ATN) Applications
- Conclusions

**Derived from the work activities related to NASA GRC funded support of the AEEC Aircraft Data Network Standard 664**

# Agenda

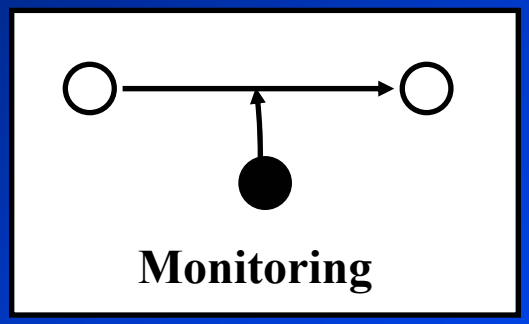


- Contemporary trends – background and the need for a defining a system engineering approach
- A security system engineering methodology
  - Report on the ongoing work of AEEC 664
- Status security related activities since 9/11
  - ICAO ATN
  - AEEC
  - RTCA
- Remarks on aviation industry PKI

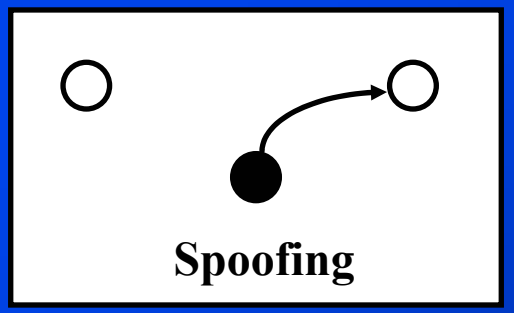
# *Why Security? CNS Data Link Threats*

*Accelerating CNS*

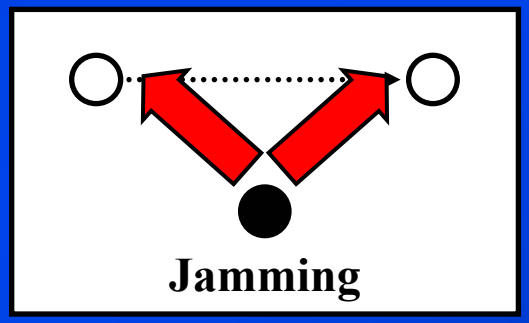
**Privacy**



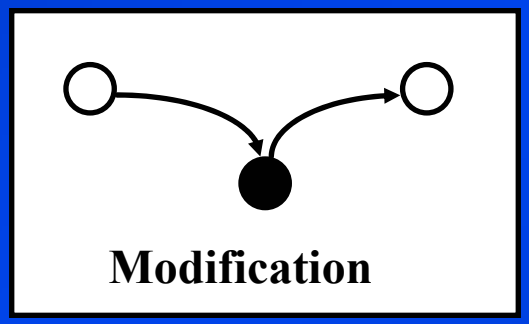

**Authentication**



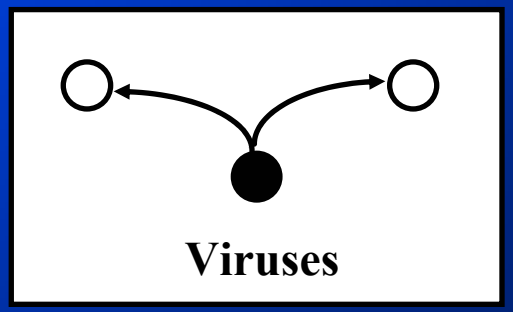

**Denial of Service**




**Integrity**

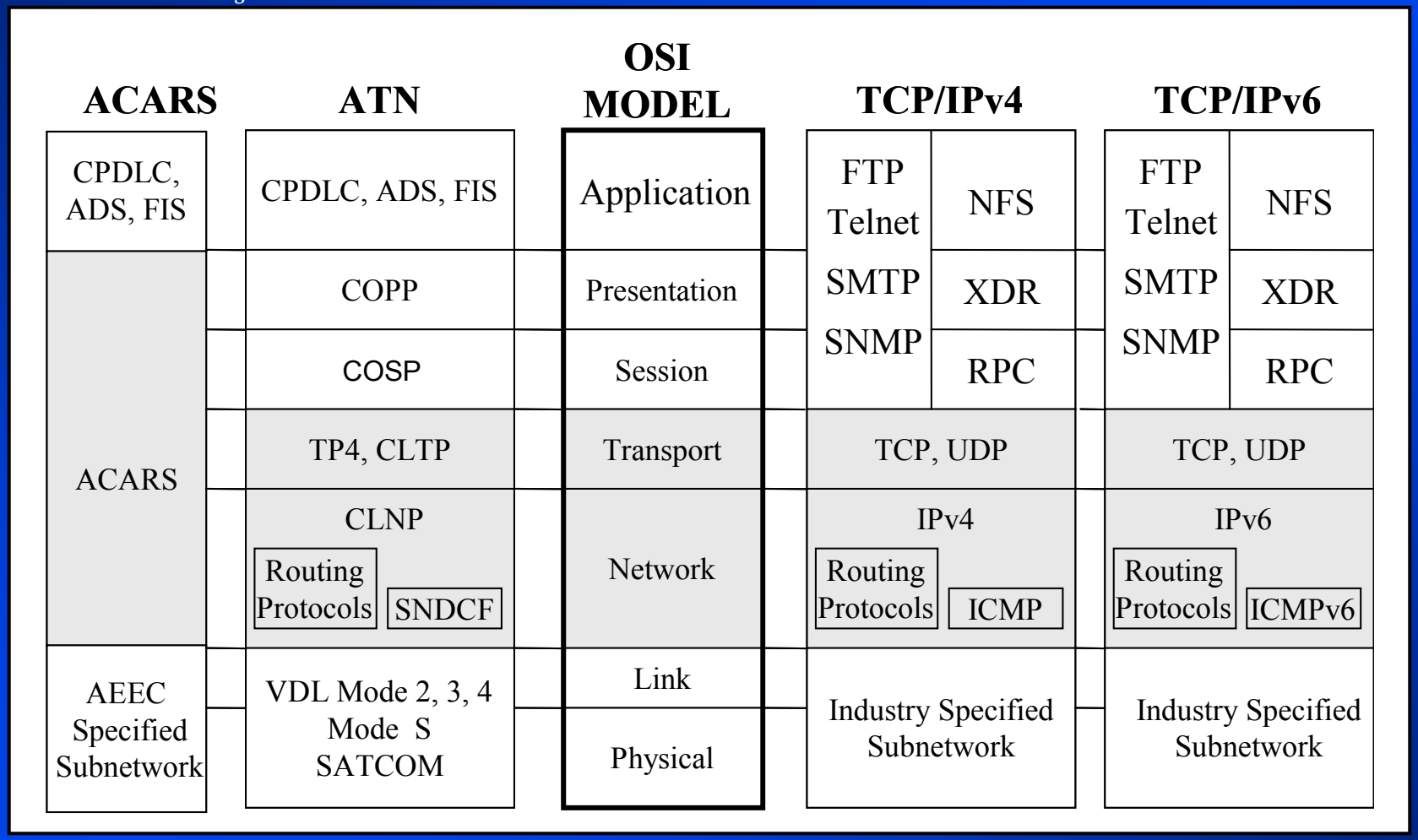



**Data Corruption**



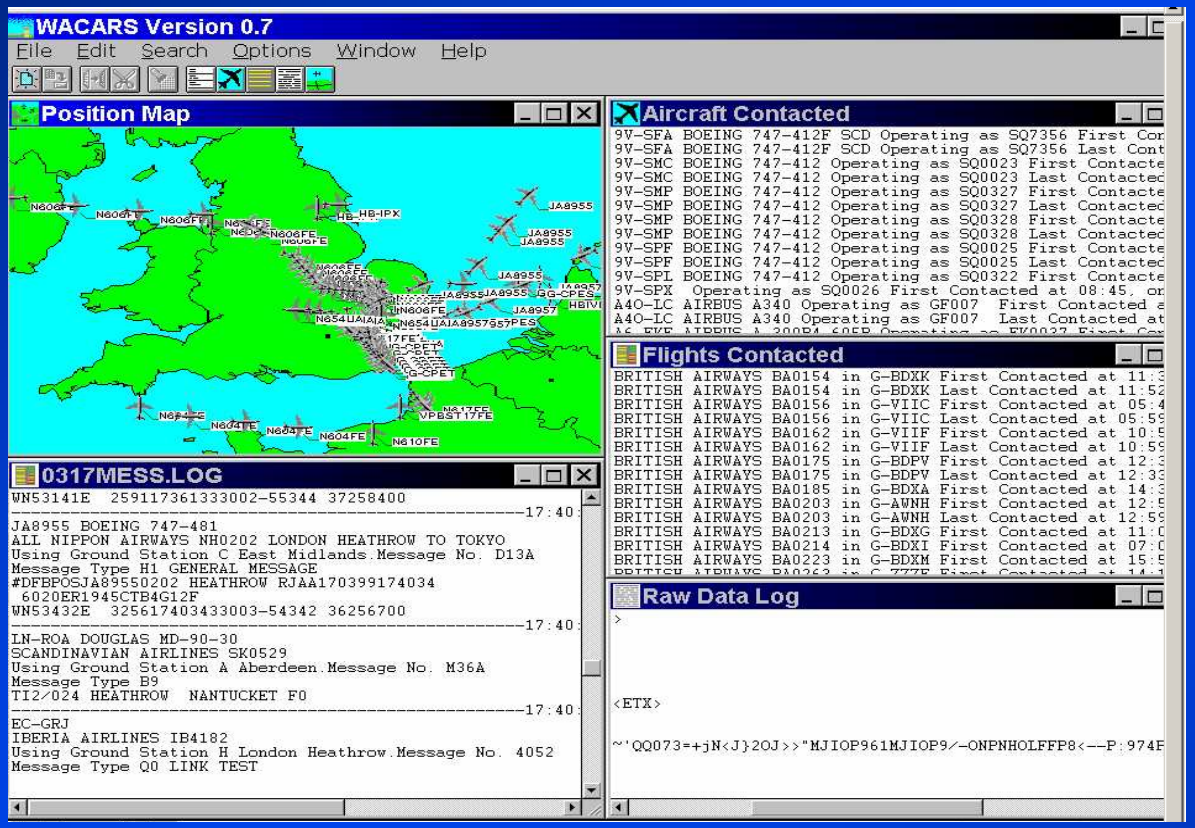
# Framework for Interoperability

*Accelerating CNS*



# Easy monitor ACARS Datalink Messages

*Accelerating CNS*




## What's Disclosed?

- Graphical Position Reports
- Contact Reports
- Detailed Message Logs

## Denial of Service

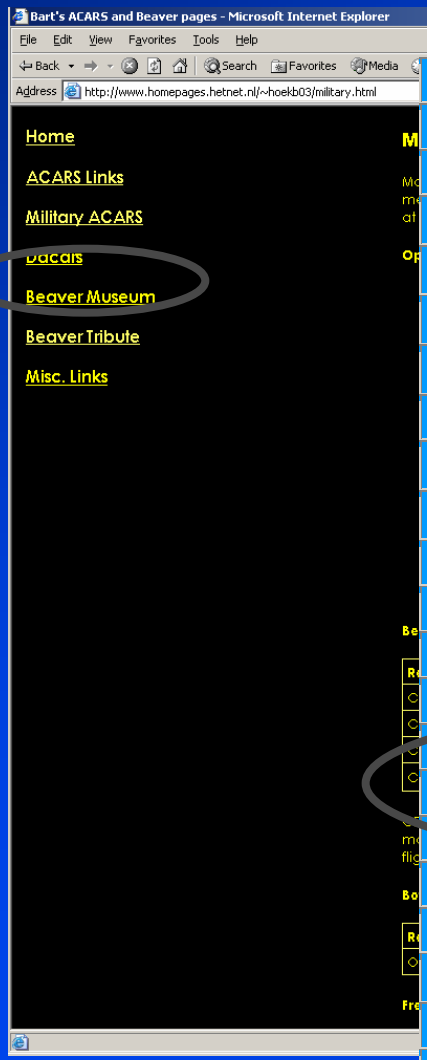
- Easily jammed

***A Personal Computer RF Scanner and Readily Available Freeware are all that is Needed***

**Courtesy James McMath, Titan Corporation**

# Military ACARS Internet Monitoring Site

*Accelerating CNS*




| ACARS | Reg. | Flightnr | Type | Unit | Homebase | last noted |
|---|---|---|---|---|---|---|
| S70400 | 97-0400 | GS0001 | C-37A | 89 AW | Andrews AFB | 02-08-2001 |
| S70401 | 97-0401 | GS0001 | C-37A | 89 AW | Andrews AFB | 23-09-2002 |
| 02-0201 | 02-0201 | | C-40C | | | - |
| 02-0202 | 02-0202 | MC#### | C-40C | | | - |
| 02-0203 | 02-0203 | | C-40C | | | - |
| 02-0204 | 02-0204 | | C-40C | | | - |
| 90402 | 99-0402 | GS0001 | C-37A | 76 AS SHAPE | Chievres (Belgium) | 24-11-2002 |
| 90404 | 99-0404 | GS0001 | C-37A | | | 14-04-2002 |
| 90405 | 99-0405 | GS0001 | C-37A | | | - |
| 98-0001 | 98-0001 | - | C-32A | 89 AW | Andrews AFB | - |
| 98-0002 | 98-0002 | MC0091 | C-32A | 89 AW | Andrews AFB | 13-07-1998 |
| 99-0003 | 99-0003 | - | C-32A | 89 AW | Andrews AFB | - |
| 99-0004 | 99-0004 | - | C-32A | 89 AW | Andrews AFB | - |
| - | 82-8000 | - | VC-25A | 89 AW | Andrews AFB | 11-2002 |
| - | 92-9000 | - | VC-25A | 89 AW | Andrews AFB | 26-0 -2002 |
| 10028 | 01-0028 | GS0001 | C-37A | 6 AW / 310 AS | McDill AFB | 08-03-2001 |
| 10029 | 01-0029 | GS0001 | C-37A | 6 AW / 310 AS | McDill AFB | 25-09-2002 |
| 10030 | 01-0030 | GS0001 | C-37A | 6 AW / 310 AS | McDill AFB | 11-10-2002 |
| 10065 | 01-0065 | GS0001 | C-37A | | | - |
| 10076 | 01-0076 | GS0001 | C-37A | 6 AW / 310 AS | McDill AFB | 27-11-2002 |
| | 00-0015 | | C-40B | Boeing | | - |

**Courtesy James McMath, Titan Corporation**

# *What is Security?*



**Not just a data link issue - security is not an add-on.**

- **Technical**
  - **Functionality, Architecture, and Design**
- **Organizational**
  - **Definition, Separation, "Need to Know"**
- **Procedural**
  - **Identification, Authentication, Limitation, Observation**

**Security must be built into the system or integrated systems design.**

# E(IP)-Enabled Aircraft - Motivation



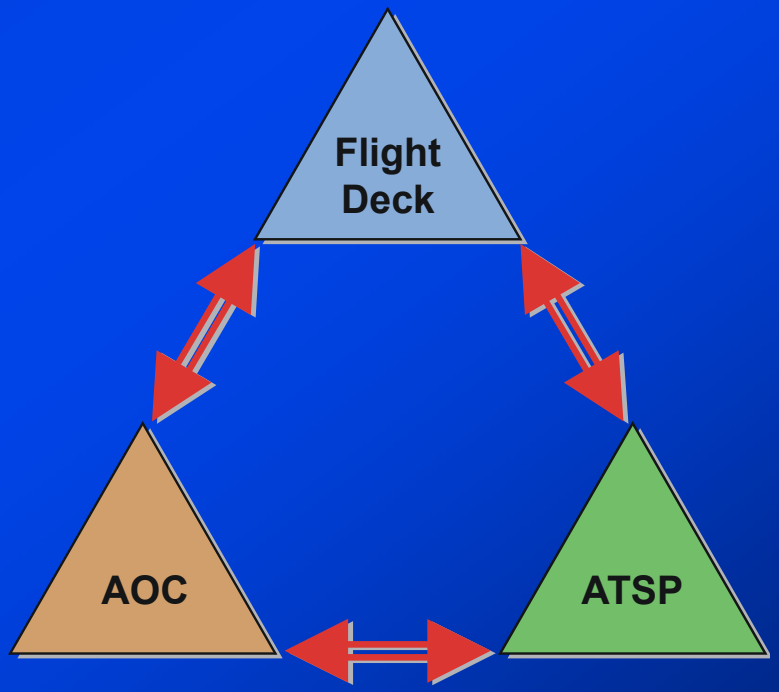
- Business process integration and more automation
- Driven by passengers
- Use of mass market "open system" products
- Lower development and operational costs
- Safety
- Examples: A380, Eurocontrol ATM ground networks (iPAX), NASA Small Aircraft Transportation – Airborne Internet

**Onboard and offboard applications integrated through IP-based networks**

# NASA Distributed Air-Ground Concepts (DAG-TM)

*Accelerating CNS*

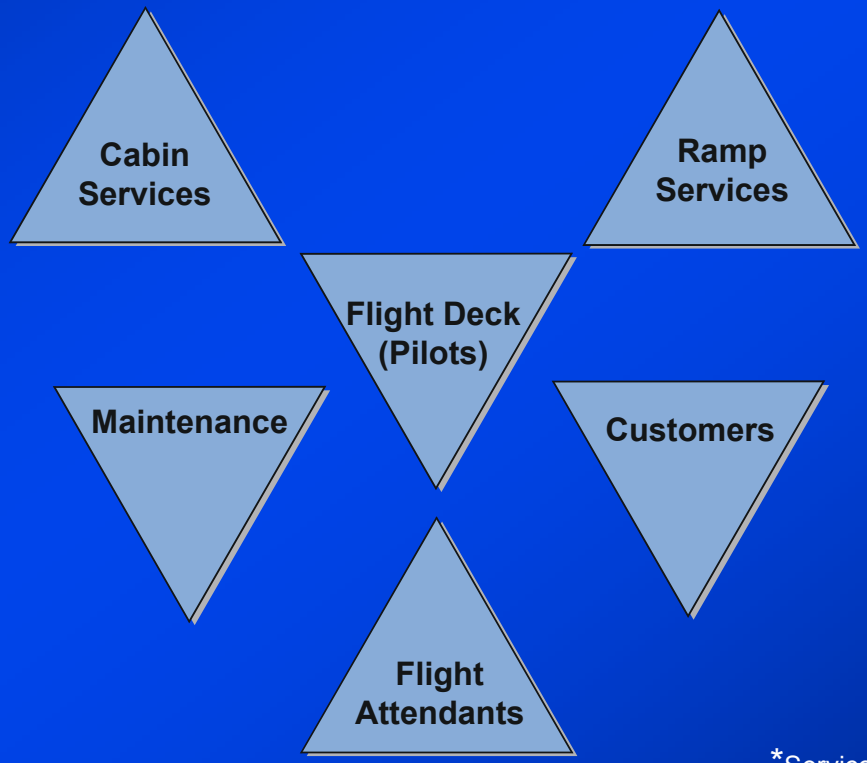
- Benefits in collaboration and integrated systems outweighs the separate and vertical systems of today
- Three Constituents
  - Airline Dispatch (AOC)
  - Air Traffic Management
  - Flight Deck
- Interconnectivity is key to business success



# DAG-TM Constituent: Flight Deck

*Accelerating CNS*

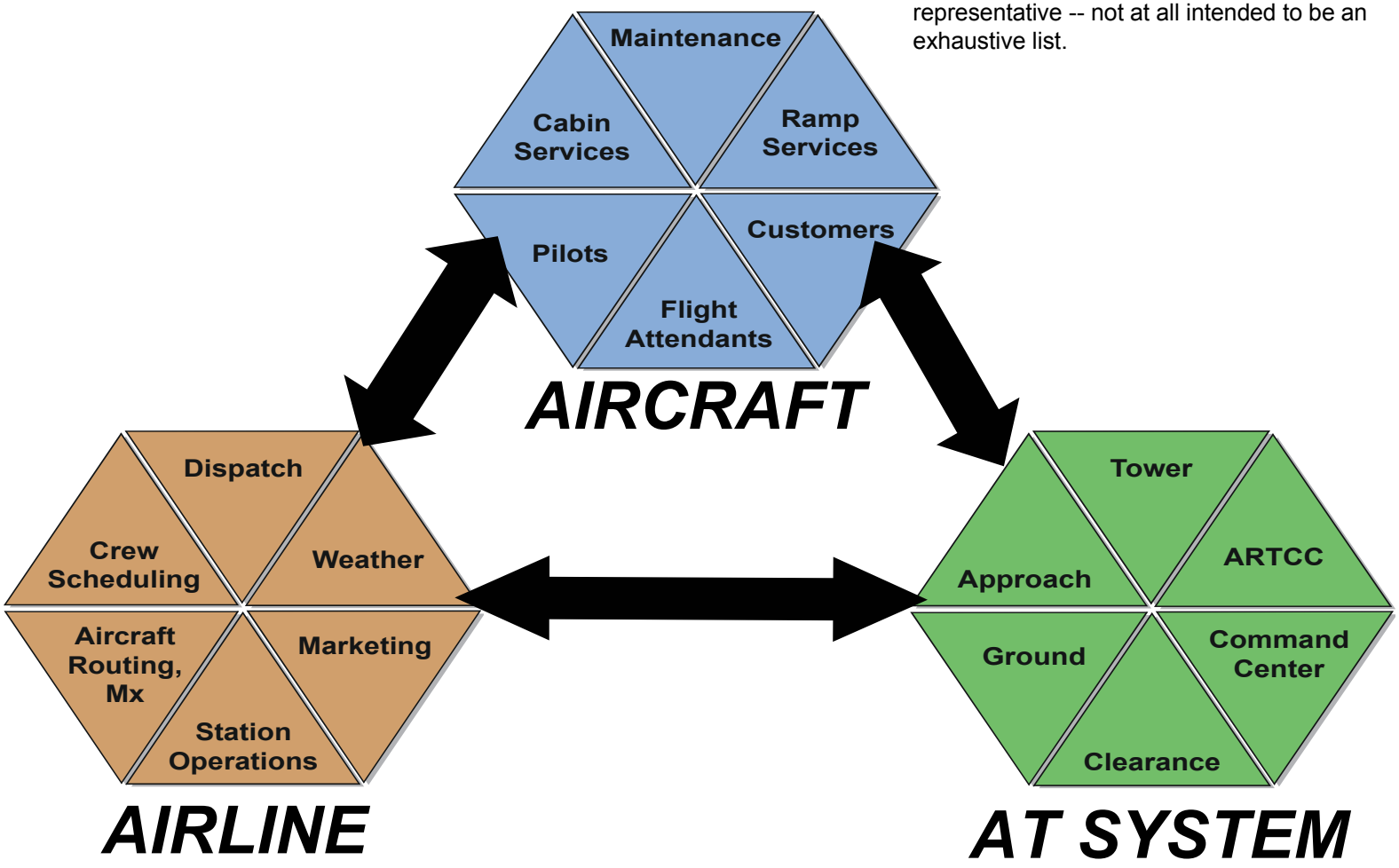
- **All Parts of the AIRCRAFT will have a voice in air commerce collaboration***




*Services/users shown are meant to be representative -- not at all intended to be an exhaustive list.

# Transition DAG-TM Constituents

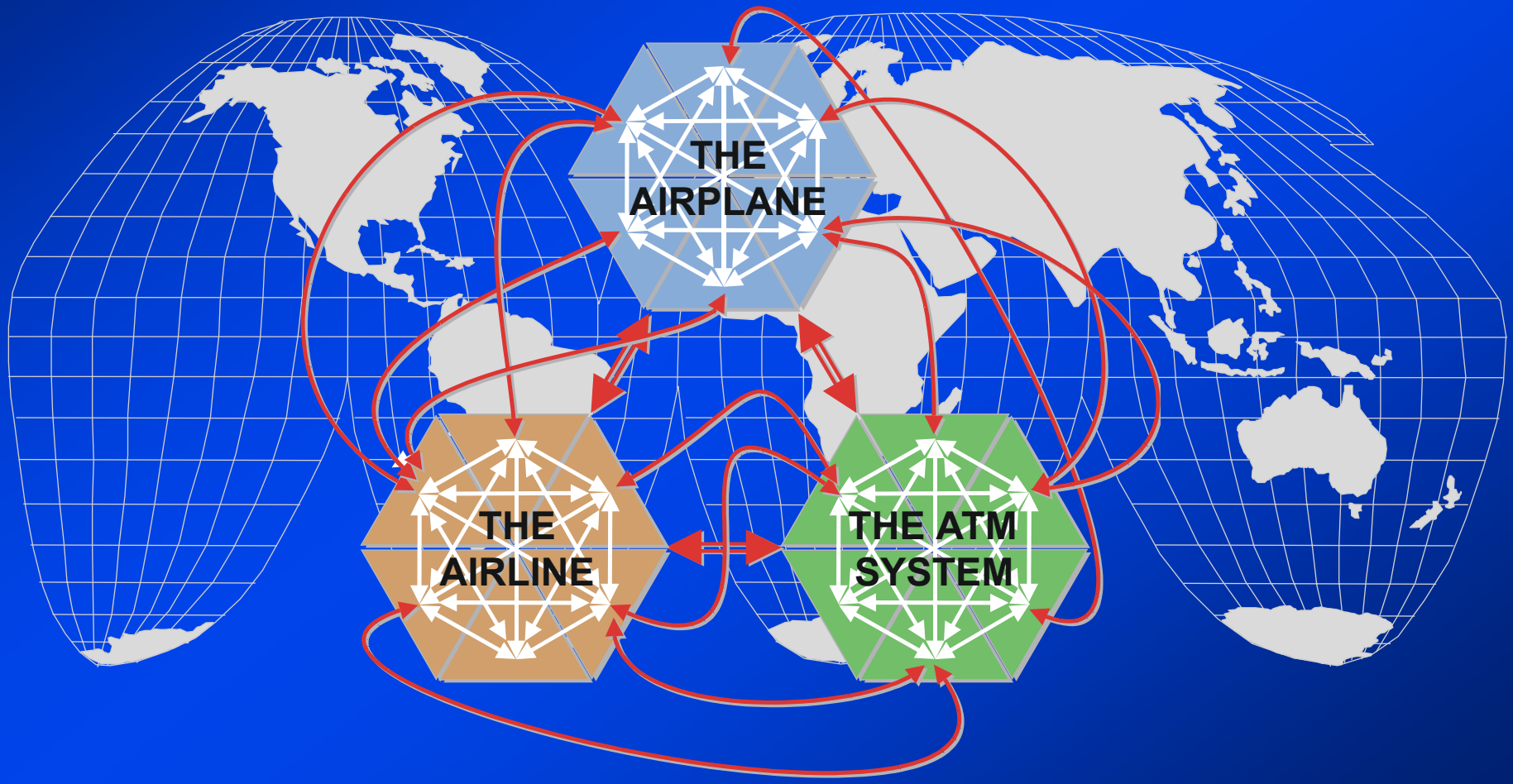
*Accelerating CNS*



# Vision

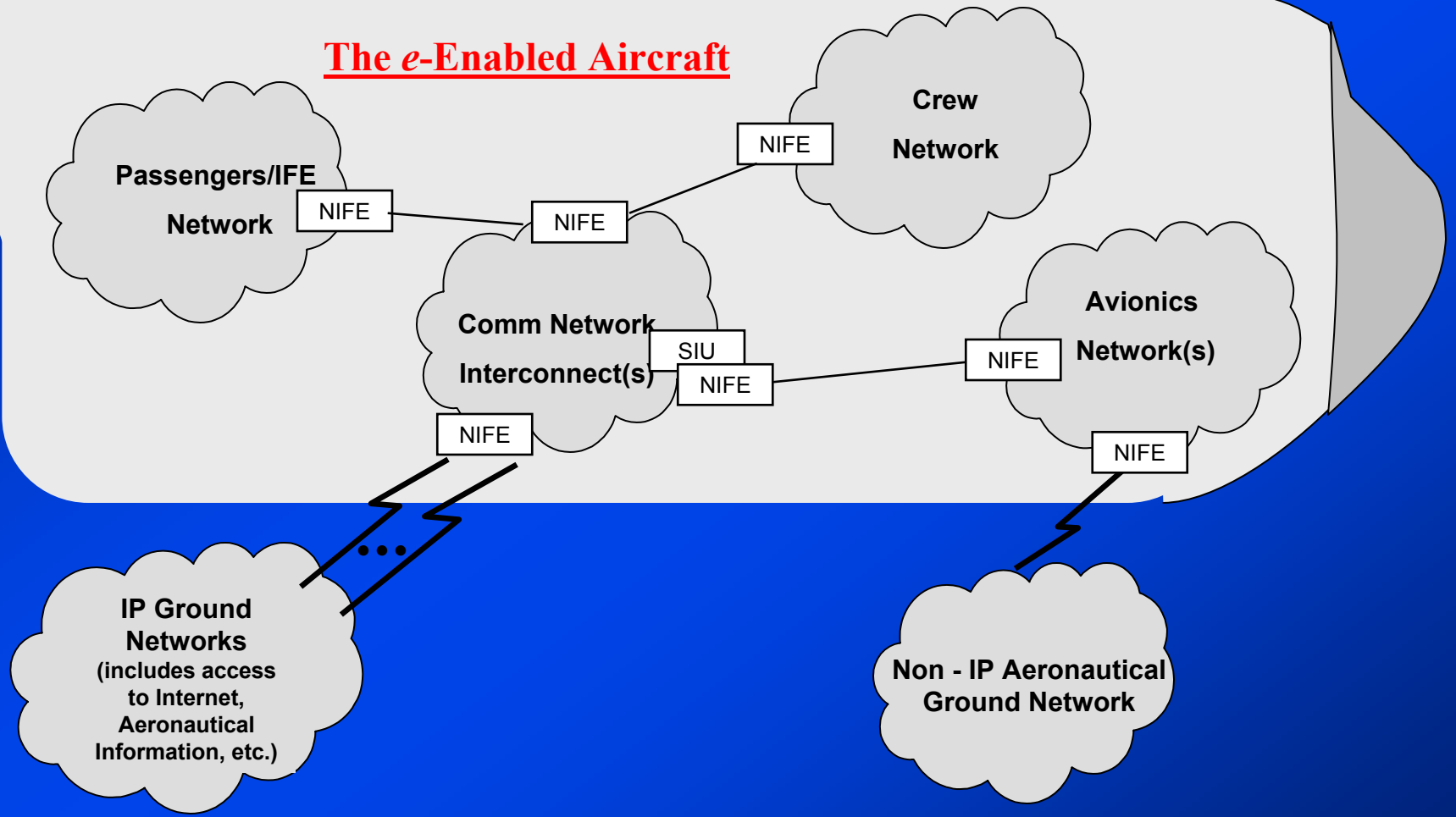


- Each constituent has multiple internal and external direct connections with the others and with the world – creating the air commerce web.



# Reference Model – Domains






NIFE = Network Interface Function Element

SIU = Secure Interface Unit

# *Before Designing – We Need Industry Consensus*

*Accelerating CNS*

- **What is our obligation about security?**
- **What is our investment in security?**
- **How do we protect that investment?**
- **What is the right design?**

**Need an industry policy covering not just ATC or just the data link, but one covering all domains.**
**Until then, we will do our best in ADN 664 Part 5**

# *Develop the Policy*

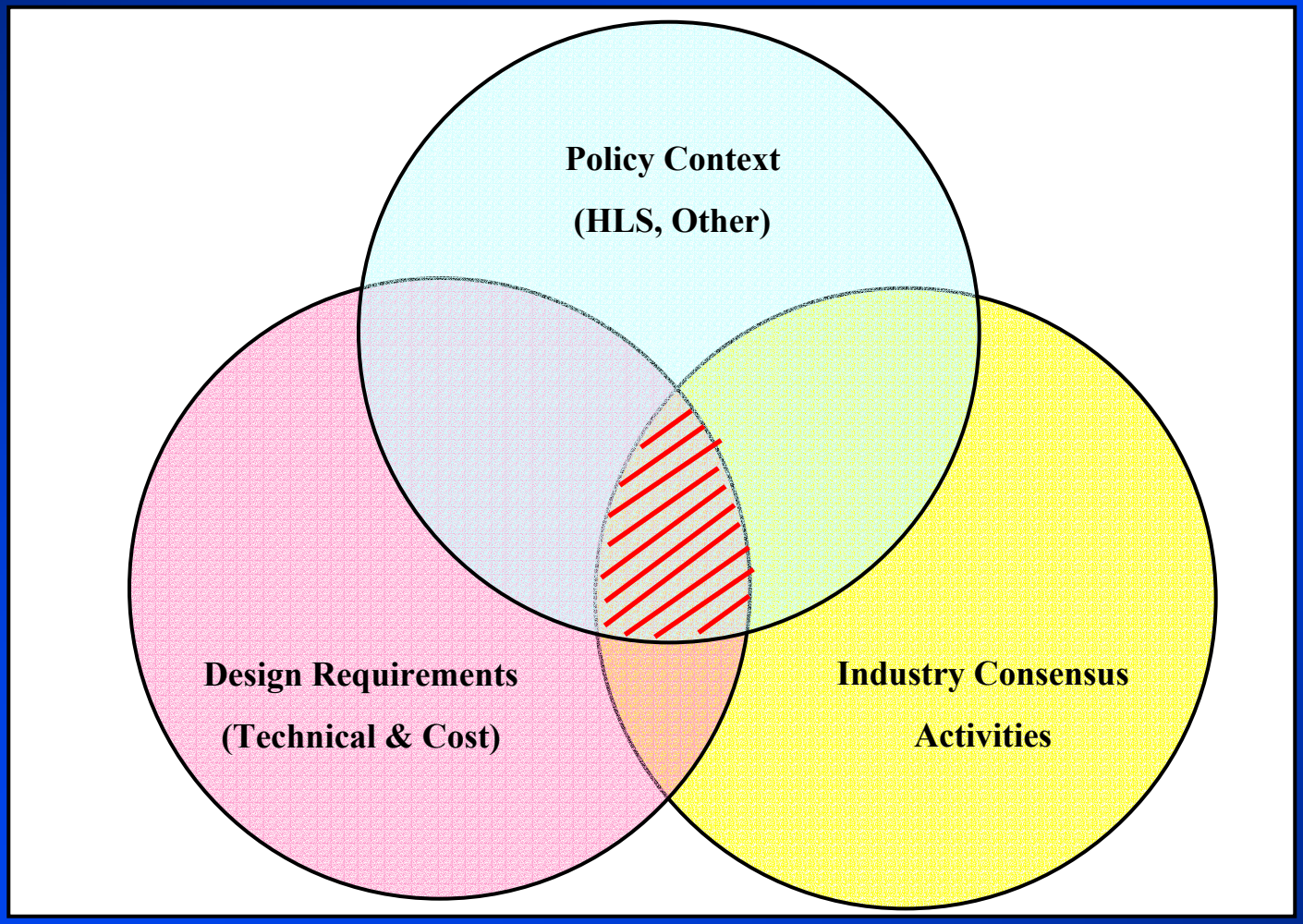


- **Analyze the Required/Desired Capabilities**
  - **Cockpit, Cabin, Maintenance, Ground Crews**
- **Define Acceptable Operational Limits**
  - **Permissible Behavior in Failure or Attack Conditions**
- **Establish Integrated Security Policies**
  - **Policies Must Comprise All Operational Areas**

**Normally this means undertaking a system engineering approach to problem solving**

# *Information Security Discussion*

*Accelerating CNS*




**The need is to develop the solution set through a system engineering approach**

# *Reference Domains - Top Level*

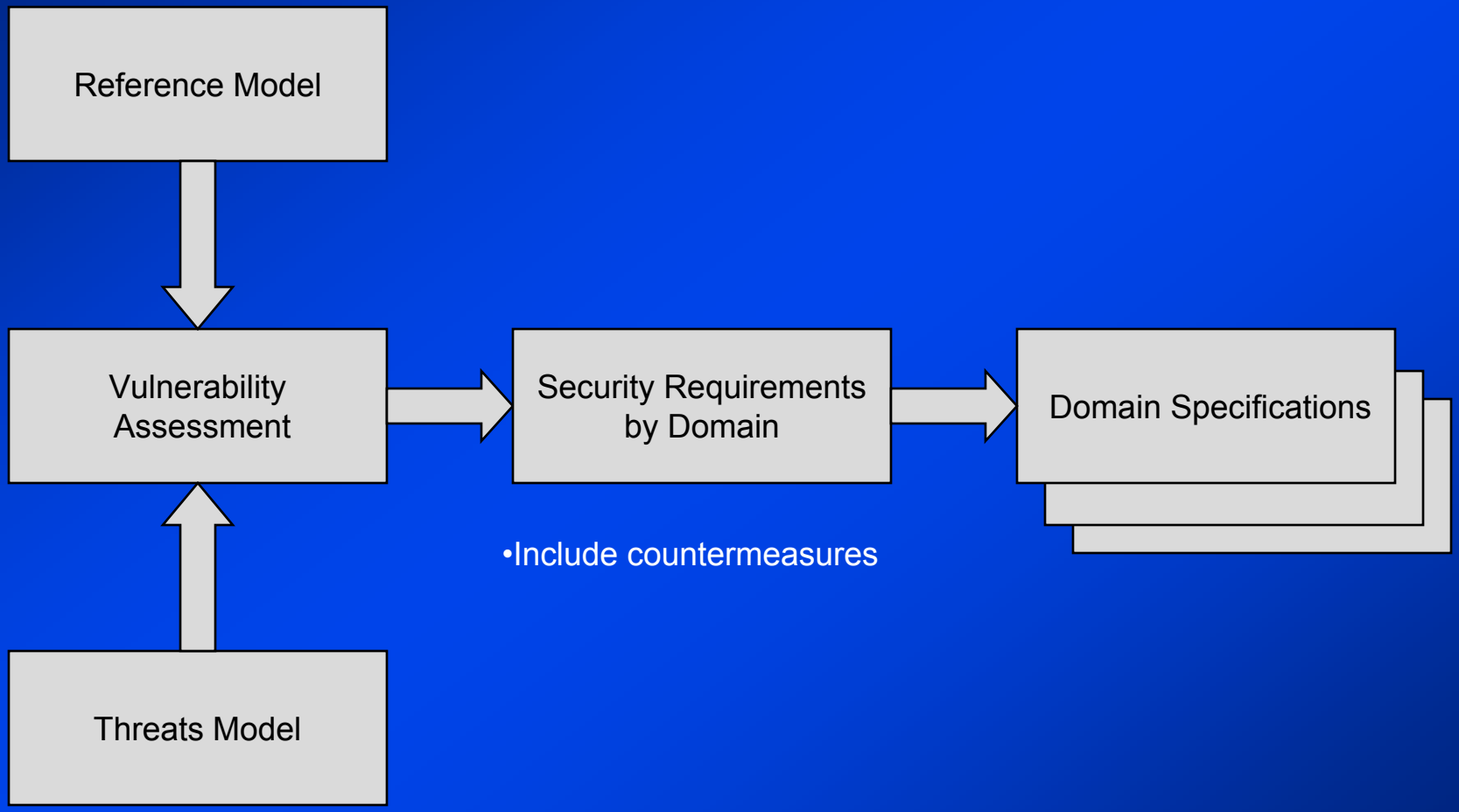


- **Onboard**
  - **Communications Network Interconnect (AEEC 763)**
  - **Crew (Crew Information System)(AEEC 763/628)**
  - **Passenger/In-flight Entertain (IFE) (AEEC 628)**
  - **Avionics (multiple) (AEEC 664)**
- **Offboard**
  - **IP-Based - Internet/VPN**
  - **Non-IP Aeronautical**
- **Must look at the security from the context of all domains and cross domains both onboard and offboard.**
- **Must look at the dataflows between trusted areas.**

# Typical Methodology

Accelerating CNS

•Consider all Domains




•Include countermeasures

•Consider Targets

# *Threat Definitions*



## Types of Threats

- Impact on life
- Impact upon property
- Impact on opportunity

## Impact of Successful Threat Action

- Grave - loss of life or injury
- Critical - injury and serious damage to property
- Some - damage to present or future resources
- Annoyance - minimal loss of time, induces stress
- Little - minor disruption
- Unknown
- None

# *Example Attack Methods*



- **Pre-production compromise (built-in back doors)**
- **Substitution of parts (Trojans in software)**
- **Code attacks (viruses)**
- **Network attacks (worms)**
- **Denial of Service attacks**
- **System specific attacks (OS vulnerability)**
- **Authentication bypass (theft of credentials, spoofing)**
- **Shutdown of support systems (power, AC, flight controls etc.)**
- **Disgruntled employee (malicious or paid)**
- **Content exploitation (information made public, identity of crew/passengers, aircraft incidents or failures)**

# Threat Impacts

*Accelerating CNS*

| | Success of Threat Action results in: | | | |
|---|---|---|---|---|
| **Domain/Interface** | Human User Disruption or Denial | Application Disruption or Failure | Network Disruption or Failure | End System Disruption or Failure |
| **Onboard** | | | | |
| Comm Network Interconnect (CNI) | Up to critical | Some | Critical | Critical |
| Crew (non-pilot) | Some | Some | Critical | Critical |
| Passenger/ In-Flight Entertainment (IFE) | Annoyance | Annoyance | Revenue Related (Some) | Future Revenue (Some) |
| Avionics | Grave | Grave | Grave | Grave |
| **Offboard** | | | | |
| IP-Based, Aeronautical (non-ATC) and Internet | Critical Annoyance | Some Annoyance | Critical Annoyance | Critical Annoyance |
| Aeronautical Non IP-Based | Grave | Critical | Critical | Critical |
| **Interfaces (cross-domain)** | | | | |
| IP Ground Network (GN) to CNI | Up to critical | Up to critical | Up to critical | Up to critical |
| Non-IP Aeronautical Ground to Avionics | Up to grave | Up to grave | Up to grave | Up to grave |
| IP GN Internet to Passenger/IFE | Some | Some | Some | Some |
| CNI to Avionics | Grave | Grave | Grave | Grave |
| CNI to Crew | Critical | Some | Some | Some |
| CNI to Passengers/IFE | Some | Some | Some | Some |
| Passenger/IFE to Avionics | Annoyance | Annoyance | Annoyance | Annoyance |
| Crew to Avionics | Critical | Some | Some | Some |

# *Network Security Services/Functions*

- **F1: Authentication**
- **F2: Access**
- **F3: Data Confidentiality**
- **F4: Data Integrity**
- **F5: Non-Repudiation**
- **F6: Intrusion Protection Methods**
- **F7: Counter Measures**
- **F8: Recovery of System/Operation**
- **F9: Logging**

# Network Security Sub-functions



- F1: Authentication
  - F1.1: Validity Checking
  - F1.2: Protection of Stored Validity Data
  - F1.3: Confidentiality of Data in Transit
  - F1.4: Additional Security Measures
- F2: Access
  - F2.1: Access Control
  - F2.2: Access List Administration
- F3: Data Confidentiality
  - F3.1: Encryption
  - F3.2: Key Distribution and Management
  - F3.3: Level of Security
  - F3.4: Layer of Encryption (Physical, Network, Higher)
  - F3.5: Encryption Application Program Interface (API)

# Security Sub-functions (cont..)



- F4: Data Integrity
  - F4.1: Acceptable transmission error
  - F4.2: Anti-Spoofing/Message Digests
  - F4.3: Key Distribution and Management
- F5: Non-Repudiation
  - F5.1: Confirmation
  - F5.2: Retention of Confirmation
  - F5.3: Key Distribution and Management
- F6: Intrusion Protection Methods
  - F6.1: Bastion Host
  - F6.2: Filters
  - F6.3: Application Gateway (Proxy Server)
  - F6.4: Internal Domain Name Server (DNS)

# Security Sub-functions (cont..)

- **F7: Counter Measures**
  - **F7.1 Protection**
    - » Denial of service, code (virus), network (worms), Trojan software
  - **F7.2 Detection**
  - **F7.3 Response**
- **F8: Recovery of System/Operation**
- **F9: Logging**

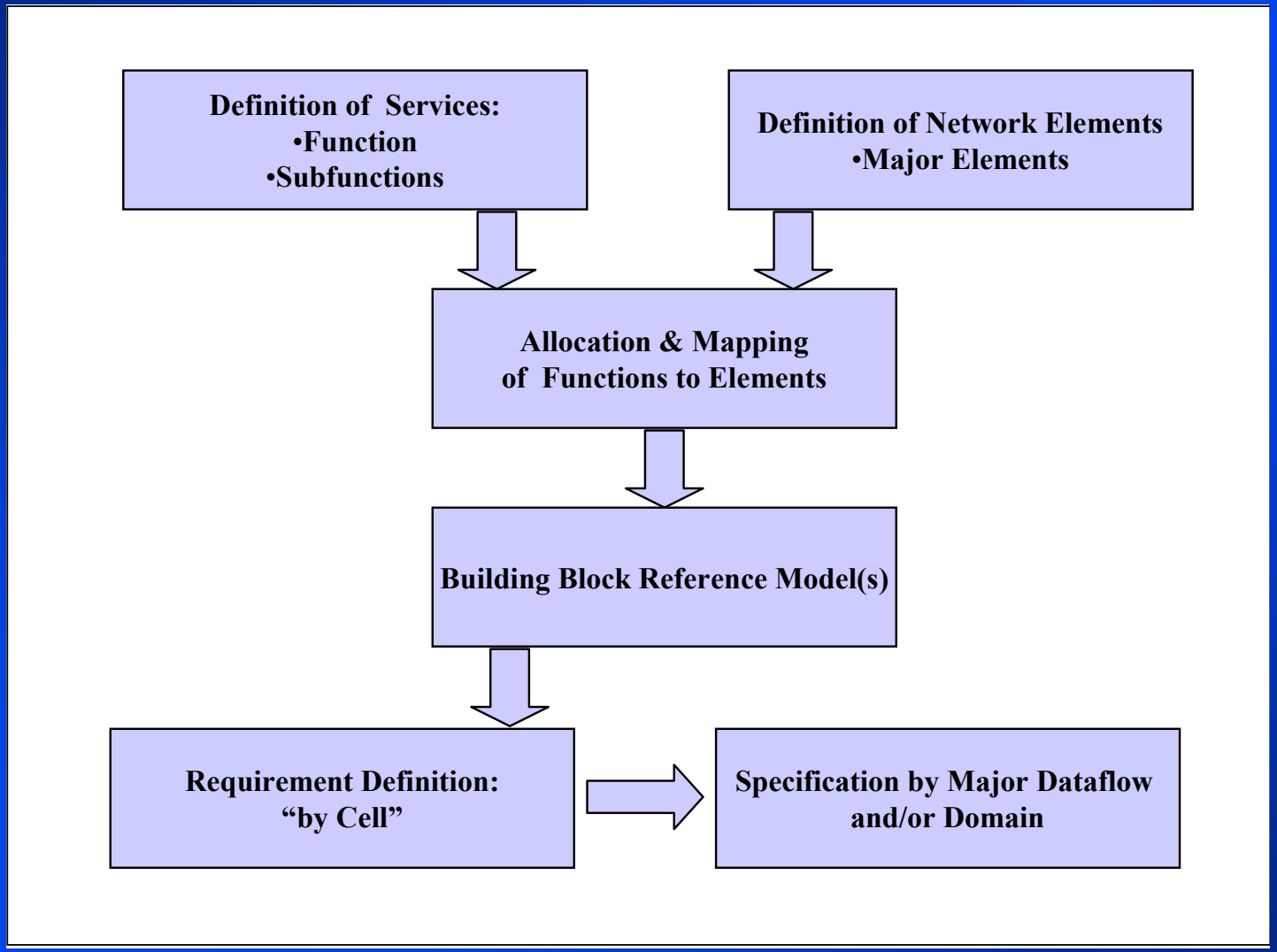
# Assessment Matrix Example (Key Dataflows )

*Accelerating CNS*

| Security Function/ Sub-function | Aero IP GN To CNI | Internet To IP GN To CNI | CNI to Passengers/IFE | CNI to Crew. | CNI to Avionics | Aero Non IP GN To Avionics |
|---|---|---|---|---|---|---|
| 1: Authentication | | | | | | |
| 1.1: Validity Checking | Offboard | Offboard | Yes + Billing | Yes | Yes, Might be static | Offboard |
| 1.2: Protection of Stored Data | Yes | User Defined | User defined | Yes | Yes | Yes |
| 1.3: Confidentiality of data in transmit | Yes | User defined | User defined | Yes | Yes (AG Appls) | Yes |
| 1.4: Additional Security Measures | Maybe | No | No | No | Maybe | Maybe |
| 2: Access Control | | | | | | |
| 2.1: Control | Yes | Yes | Yes | Yes | Yes | Yes |
| 2.1: Access List Admin | Yes | Yes | Yes | Yes | Yes | Yes |
| 3: Data Confidentiality | | | | | | |
| 3.1: Encryption | Yes | User Defined | User defined | Yes | Yes | Yes |
| 3.2: Key Distribution and Management | Yes | User defined | User defined | Yes | Yes | Yes |
| 3.3: Level of Security | Yes | No | No | No | Yes | No |
| 3.4: Layer of encryption | | | | | | |
| 3.4.1: Physical | No | No | No | No | No | No |
| 3.4.2: Network | Yes | User defined | Yes | Yes | Yes | Yes |
| 3.4.3: Higher Layers | No | User defined | User defined | No | No | Yes |
| 3.5: Encryption API | No | No | No | No | No | No |

# Internetworking Architecture Analysis

*Accelerating CNS*



# *Building Block Reference Model*

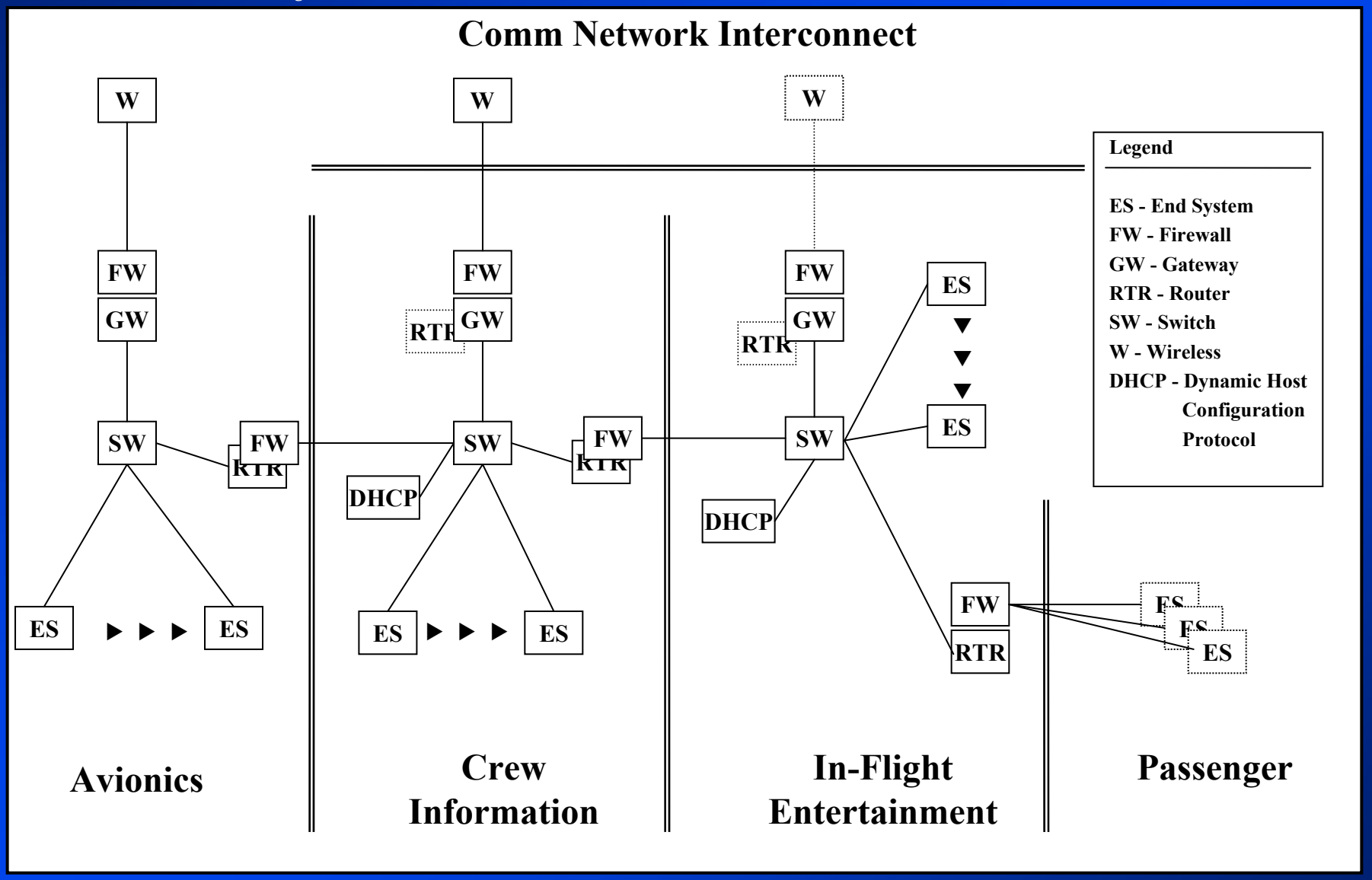


- **View each domain as a set of Network Functional Elements (NFEs).**
- **Analyze the dataflows between domains.**
- **Specify the requirements for the services performed by each NFE in the dataflow between trusted areas.**
- **Understand the operational impacts and costs.**

**Reads similar to the "COMMON Criteria" approach**

# Building Block Reference Model

*Accelerating CNS*



# Network Security Functional Elements

*Accelerating CNS*

| | Authentication | Access | Data Confidentiality | Data Integrity | Non-Repudiation | Intrusion Protection Methods | Counter Measures | Recovery of System / Operation | Logging |
|---|---|---|---|---|---|---|---|---|---|
| End System (or DTE) | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Autoconfigure / Loader | - | - | - | - | - | - | - | - | - |
| Certification Authority | ● | - | ● | ● | ● | - | - | - | ● |
| DHCP | - | - | - | ● | - | - | - | - | ○ |
| DNS | ○ | - | - | ● | - | ● | - | - | ○ |
| Network Management Station | ● | ● | ● | ● | ● | - | - | - | ● |
| Firewall | ● | ● | ⊙ | ● | ⊙ | ● | ● | - | ● |
| Gateway | ⊙ | ● | ⊙ | ● | ⊙ | ● | ● | - | ○ |
| Router | ⊙ | ● | ⊙ | ● | ⊙ | ● | ● | - | ○ |
| Access Point | ⊙ | ⊙ | ● | ⊙ | ⊙ | ⊙ | - | - | - |
| Bridge (or Switch) | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ | - | - | ● |
| Backbone | ○ | ○ | ⊙ | ⊙ | ⊙ | ⊙ | - | - | - |
| Cable Plant | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ | - | - | - |
| Repeater (or Hub) | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ | - | - | - |

| Legend | Meaning |
|---|---|
| - | Not Applicable |
| ○ | Optional |
| ⊙ | Present, but not required for a special task |
| ● | Present, required for a special task |

# Security Sub-functions – Authentication

*Accelerating CNS*

| ***F1: Authentication*** | *F1.1: Validity Checking* | *F1.2: Protection of Stored Validation Data* | *F1.3: Confidentiality of Data in Transit* | *F1.4: Additional Security Measures* |
|---|---|---|---|---|
| *End System (or DTE)* | ● | ● | ● | ○ |
| *Certification Authority* | ● | ● | ● | ○ |
| *Network Management Station* | ● | ● | ● | ○ |
| *Firewall* | - | - | ● | - |

| *Legend* | *Meaning* |
|---|---|
| - | Not Applicable |
| ○ | Optional |
| ⊙ | Present, but not required for a special task |
| ● | Present, required for a special task |

# Security Sub-functions – e.g.,Authentication


*Accelerating CNS*

| ***F1: Authentication*** | *F1.1: Validity Checking* | *F1.2: Protection of Stored Validation Data* | *F1.3: Confidentiality of Data in Transit* | *F1.4: Additional Security Measures* |
|---|---|---|---|---|
| *End System (or DTE)* | Shall require valid UserID/Password combination to access Network services. | May store passwords locally; if so, these passwords shall be stored in an encrypted format. | Shall encrypt sensitive information (e.g. passwords) before transmitting through the network. | May employ additional security measures (e.g. smart cards, single-use passwords). |
| *Certification Authority* | Shall validate credentials before performing services for a user. | May store passwords and private keys locally; if so, these shall be stored in an encrypted format. | Shall encrypt sensitive information (e.g. passwords, private keys) before transmitting through the network. | May employ additional security measures (e.g. smart cards, single use passwords). |
| *Network Management Station* | Shall require valid UserID/Password combination to access the system. | May store passwords locally; if so, these shall be stored in an encrypted format. | Shall encrypt sensitive information (e.g. passwords) before transmitting through the network. | May employ additional security measures (e.g. smart cards, single use passwords). |
| *Firewall* | - | - | Shall apply filters to prevent sensitive data from crossing into publicly accessible domains. | - |

# Next Steps



- **Break down the End-to-End communications process by potential information flow and describe what services are required for each flow.**
- **Potential endpoints to consider include IP and Non-IP Ground systems, the Avionics and Pilot, the Crew, and the Passengers**
  - **Ground IP → Avionics**
    - AOC, Weather
  - **Ground Non-IP → Avionics**
  - **Avionics → Crew**
  - **Ground IP → Crew**
  - **Ground IP → Passenger**
- **SEEK ANALYSIS FUNDING SOURCES**

# ATN Standards and Recommended Practices (SARPs)


*Accelerating CNS*

- Document 9705, Ed 3, October 2002 Sub-Volume VIII
- Risk analysis performed by Eurocontrol has identified the following threats:
  - Masquerade/modification/replay of air-ground application communications.
  - Denial of service by flooding ground IDRP databases.
- ATN SARPs (Edition 3) provides the following security services:
  - Authentication and integrity of air-ground applications.
- Authentication and integrity of IDRP communications.
  - Supporting Public Key Infrastructure (PKI).
- Airlines desire to ensure the confidentiality of operational data.
- ATNP WG-B/Sub-Group 3 is enhancing the ATN SARPs to add confidentiality services (ed. 4)

# AEEC Ad Hoc Meeting on Security – 03/7-9/02



- Several Presentations by interested agencies
  - Many agencies looking at security
  - Meeting attendees agreed – now's the time to look at standards development
- Opportunities exist for either Data Link Service Provider (DSP) or End Agency User solutions
  - Based on user requirements and cost benefits
- ATN security is the baseline – ACARS security should be compatible with/conform to ATN security requirements.
  - Bottom Line – don't build an ACARS only solution!

# Ad Hoc Meeting Conclusions



- Meeting report published on ARINC Website
  - http://www.arinc.com/aeec/projects/dlk_systems/security/index.html
- Consensus reached on report conclusions
  - Data Link Security is a Concern
  - At Least One Potential Solution for ACARS and ATN in Development
  - Problem with distribution of Threat and Vulnerability Information – AEEC Charter is Open Information
  - AEEC Must Coordinate with Other Organizations
  - Early Considerations will Minimize Future Costs

# AEEC



- Requested that Service Providers and Avionics Vendors get together to find legacy system approach (closed sessions)
- ARINC Standards/Project Improvement Modification (APIM) 02-002. Responds to ATN Panel Letter
  - Requests AEEC Investigate Key Management and Distribution
  - Develop AEEC Standard
- Accepted by AEEC General Session (2002)
  - Assigned Category 1 Priority (Authorized)
  - Assigned to:
    - Data Link Users Forum
    - Data Link System Subcommittee

# RTCA SC-201



- Chartered in Sept 2002
- The FAA position is that ACARS operational approval now includes messages which directly impact safety and regularity of flight (i.e., AOC data link ACARS does not meet published FAR means of compliance for hardware and software which support these AOC messages) - in other words ACARS is operating above is design assurance level
- Weight and Balance messages contain:
  - Zero Fuel Weight (ZFW)
  - Gross Take Off Weight (GTOW)
  - GTOW Center of Gravity (C.G.)
- Takeoff Data in messages contain:
  - V-Speeds: V1 / VR / V2
  - Flap setting
- Committee Main Focus in software assurance level
  - Other data link data not in focus

# The Approach Summary ADN Part 5



- Need to develop a clear threat assessment.
- Need to develop Aviation Industry (may be the AEEC) Security Policy that is applicable to all domains or wait for the HLS to organize it?
- Develop specific security design
  - Separate security domains onboard
  - Relative levels of security per domain
  - Functional limitation between domains
  - Definitive operational predetermination
  - Define procedural and administrative rules
- Awaiting ADN Committee direction
- Key to the statement of requirement is the understanding of the security design/features available in today's protocols

# *Security Services ATN and IP*



- **Key Management**
- **Confidentiality**
- **Non repudiation**
- **Integrity/Authentication**
- **Authorization**

**Key Issue:**

- **Where (protocol layer) to provide these services**

# ATN Security Services



**Goal:**

- **Secure exchange of ATS information**
- **Protection against unauthorized access**

**ATN Security Services:**

- **Access Control**
- **Authentication**
- **Data Integrity**

# ATN Security Services (cont.…)

CNS

*Accelerating CNS*

- **Message Authentication**
  - **64 bit key between peer entities**
  - **Message Authentication Check (MAC) in each message**
- **Replay Protection**
  - **Unique Message ID or Sequence number for the life time of key**
- **Security Label**
  - **Specified by the transport service user to be associated with TSDU**
- **IDRP**
  - **Type 1, 2 or 3 mechanisms**
  - **Type 1 is based on unencrypted checksum**
- **ATN Security Frame work - PKI**

# TCP/IP Security Services



- IP Security (IPSec)
  - Encapsulating Security Payload (ESP)
  - Authentication Header (AH)
- Authentication Header (AH) functions
  - Proof of data origin, Data Integrity, Anti Replay protection
- Encapsulation Security Payload (ESP) functions
  - AH functions + data confidentiality
- Transport Mode
  - Upper layer protocols
- Tunnel Mode
  - IP Datagrams
  - Our thesis is security at the IP layer has many advantages

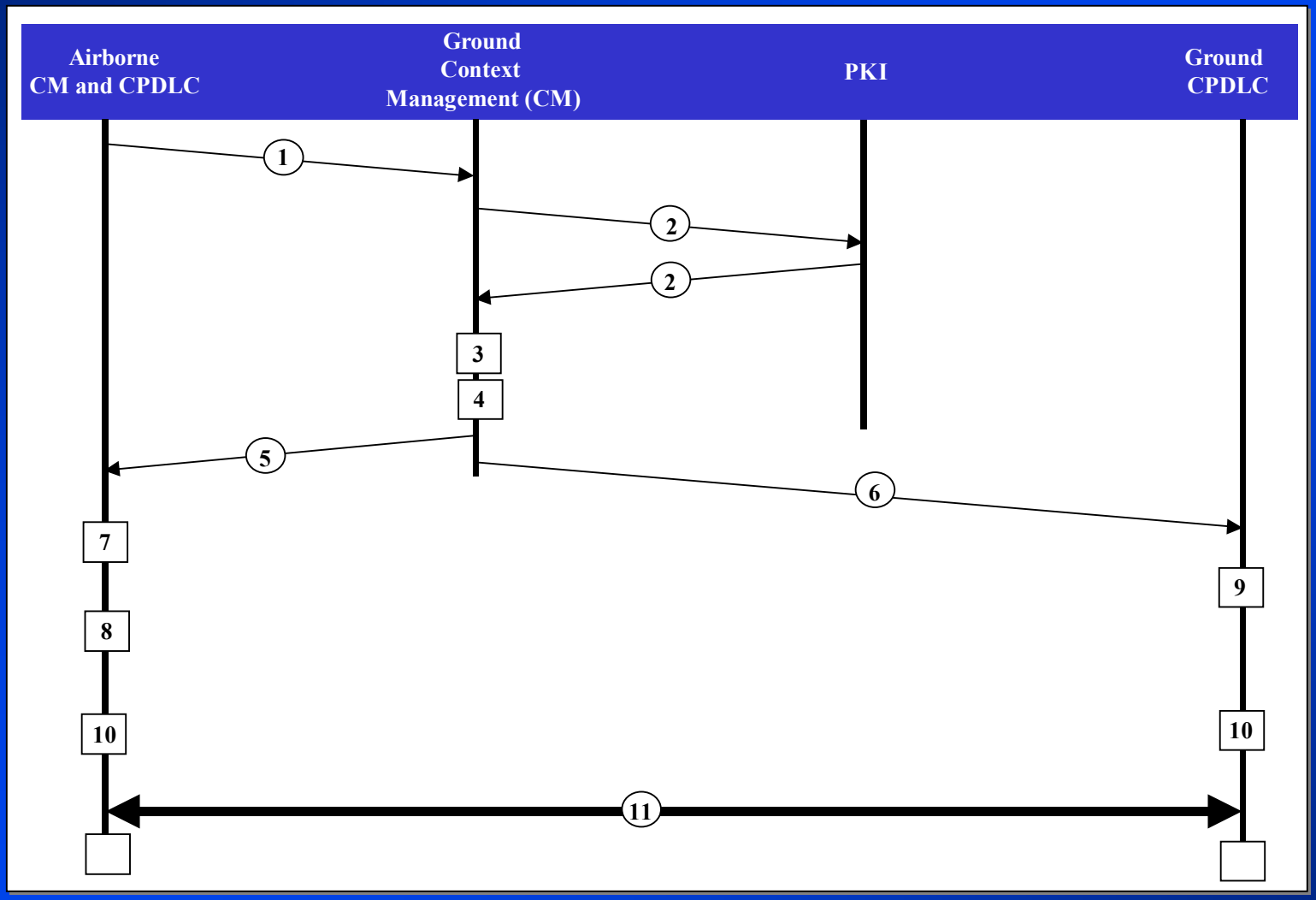
# Challenges in Specifying the Requirements



- **Getting ready for aviation applications use of or move towards an accepted aviation architecture fully based upon IP**
- **Application layer versus other layer security**
- **Final specification of PKI**
  - **Individual States determine own ATN Security Requirements**
    - » Standardization is a must do activity.
    - » Avoid Regional/individual State implementations.
  - **Key Pairs must change every 28 days**
    - » Same cycle as Navigation Data Base uploads.
    - » Private Keys must be protected.
    - » Public Keys must be distributed according to owning CA prerogatives.
  - **Airframe has only 2 key pairs for all ATN applications**

# PKI in a Secure CPDLC Environment

*Accelerating CNS*



# *Public-key Cryptography*



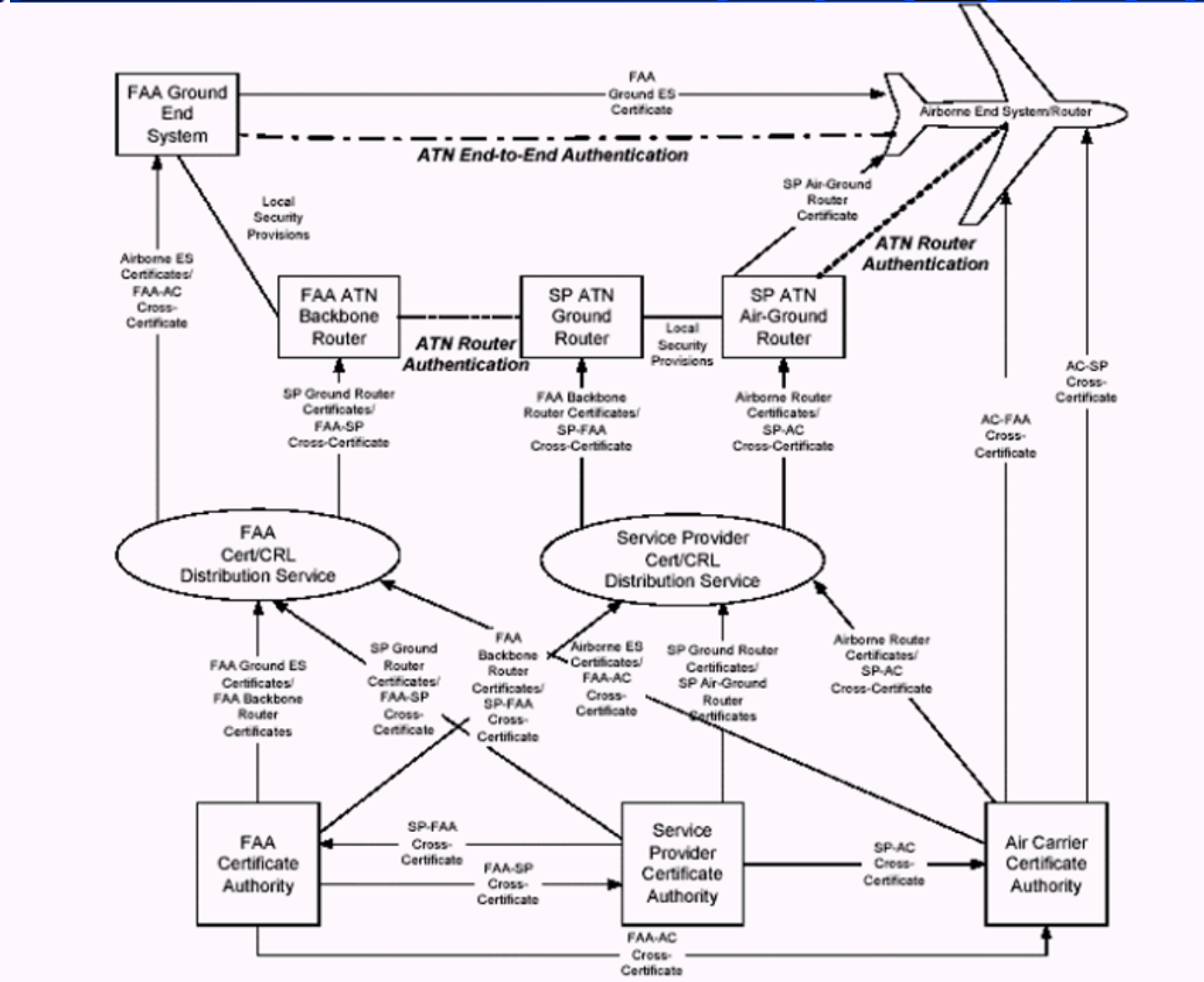
- **In a public-key cryptographic scheme, each user has two keys known as a key pair. One key is public, the other is private.**
- **The mathematical relationship between the keys ensures knowledge of public key does not compromise private key.**
- **Public-key encryption schemes provide data confidentiality. Public key signature schemes provide data integrity, data origin authentication, and non-repudiation.**

# Certification Issues



- Two types of cryptographic scheme are in use: symmetric schemes and public key schemes.
- Certification can solve the public key distribution problem. CAs can be off-line and are not unconditionally trusted.
- However CAs do take on significant liability, they have high security requirements, and they need a supporting infrastructure - a Public Key.
- Infrastructure or PKI. Furthermore, issues need to be addressed:
  - Multiple CAs.
  - Revocation.
  - Certificate size (X.509 cert size often 20K).

# Example of Certificate Environment



# PKI Issues



- Interoperability -
  - Mature API is not yet there
- Scalability
  - At present all implementations are small scale. Scalability is question
- Affordability
  - - positively identifying internal and external users, generating keys, issuing them digital certificates, and managing the exchange and verification of certificates. In addition, existing software applications, electronic directories, and other legacy systems must be modified so they can interact with the PKI.

# PKI Issues

- Policies and Procedures
  - Establishing and enforcing policies and procedures will require resolution of a range of sensitive issues.
- Trained personnel
  - Operator and technical staffs

# PKI Performance Issues



- End User Experience
- Impact of Network Performance
- Server Performance
- CA Performance Issues
  - Right sizing CPU
  - Database organization(indexing..)
  - Right sizing Memory
  - Excessive client to server communication

# *Adopt the World of Mobile IP*



- **Use the framework of IPv6**
- **Work the AAA**
- **Lead aviation requirements into IETF NEtwork MObility (NEMO) Working Group**

# Contacts

*Accelerating CNS*


**Computer Networks & Software, Inc.**
**7405 Alban Station Ct.**
**Suite B-225**
**Springfield, VA 22150-2318**

**CNS: Chris Dhas or Chris Wargo**
**703-644-2103**
**Chris.Dhas@CNSw.com, Chris.Wargo@CNSw.com**
**www.CNSw.com**